

SIL WAC AX



User Manual

TABLE OF CONTENTS

Introduction.....	5
Supported Products.....	5
Wireless Modes	5
System Requirements.....	5
Packing list	6
Configuration.....	7
Getting Started	7
System Overview	9
Dashboard	9
Network Status.....	9
Network.....	10
Status.....	11
WiFi Sta Info	11
Line Monitoring	12
Authorised Users	13
License	14
ARP List.....	14
HotSpot.....	15
Local Portal	15
<i>Display Configuration</i>	<i>15</i>
<i>Authentication Configuration – Local User.....</i>	<i>16</i>
<i>Authentication Configuration – radius Auth.....</i>	<i>17</i>
<i>Authentication Configuration – Phone Num Auth.....</i>	<i>18</i>
<i>Authentication Configuration – SMS Auth.....</i>	<i>19</i>
<i>Authentication Configuration – OneKey Auth</i>	<i>20</i>
<i>Authentication Configuration – Pre-Shared Password</i>	<i>21</i>

<i>Authentication Configuration – Vouchers</i>	22
Billing Plan	24
Local Users.....	25
Vouchers.....	26
Radius	27
SMS Gateway.....	28
White List.....	28
Black List.....	28
Wireless	29
Overview.....	29
AP Group	30
2.4GHz	31
5GHz	32
<i>Advanced</i>	33
<i>Other Configuration</i>	35
AP List	36
<i>Binding</i>	36
RF Planning.....	37
WhiteBlack List	38
Firmware.....	39
Network Topology	40
CPE Management	41
CPE Global Configuration	41
Unified Cloud	42
Unified Cloud	42
Application.....	43
UPnP Server	43
DDNS.....	44
Ngrok Client.....	45

Wake on LAN	46
Switch Linkage	47
Smart Device.....	47
Security	47
Email Notice.....	47
System	48
System Maintenance	48
User management	49
Diagnosis.....	50
Ping.....	50
TraceRoute	51
Network Tool.....	52
Telnet.....	52
System Time	53
NTP	53
Logging.....	53
Other SilverNet Products.....	54
Pro Range	54
Industrial Network Transmission.....	54
Intelligent Wi-Fi Solutions	54
Industry Leading Technical Support	54

INTRODUCTION

This User Guide is for the SilverNet SIL WAC AX AC controller.

SUPPORTED PRODUCTS

The SIL WAC AX supports the following products:

- SIL WCAP-AX
- SIL WCAP-AX-W
- SIL WCAP-AX-EXT
- SIL WCAP-AX-EXT+

For more information, visit www.silvernet.com

WIRELESS MODES

The SilverNet Access Points support the following modes:

- FAT mode

A FAT AP can provide wireless access independently.

- FIT mode

A FIT AP must be used with a controller to provide wireless access.

SYSTEM REQUIREMENTS

- Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, Linux, or Mac OS X
- Web Browser: Mozilla Firefox, Apple Safari, Google Chrome, or Microsoft Internet Explorer 9 (or above)

PACKING LIST

Please check the following items in the package before installing the device

AC Controller	1 piece
User manual	1 copy
Power Cable	1 piece
Set of brackets	1 piece
Set of screws	1 piece

Please contact your distributor immediately for any missing or damaged items.

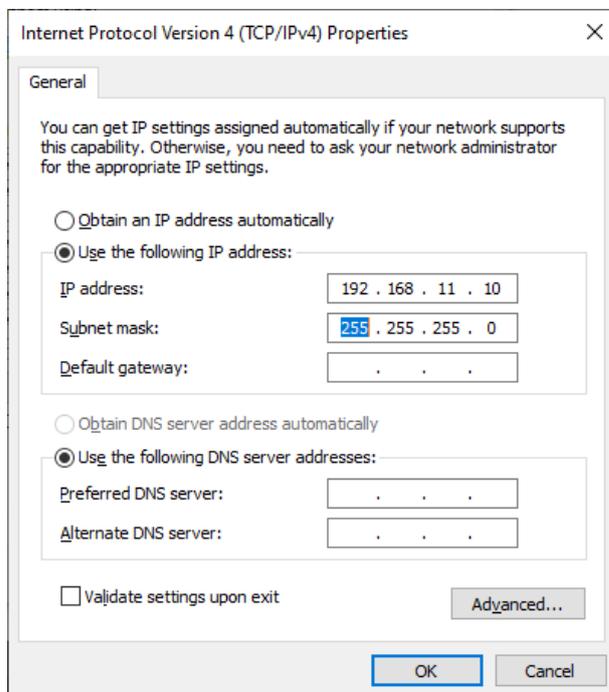
CONFIGURATION

GETTING STARTED

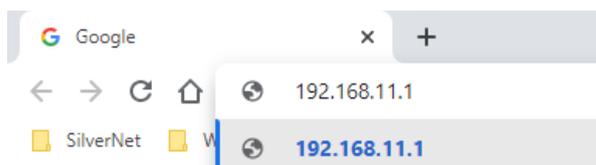
The Controller is sent out on DHCP. Once you have connected the controller to your network it is recommended you run an IP scan to check the IP address. If no DHCP server is available, then the controller will either be on 192.168.1.2 or 192.168.11.1

To access the Controllers Configuration Interface, perform the following steps:

1. Configure the Ethernet adapter on your computer with a static IP address on the correct subnet. In this example we will be using the 192.168.11.x subnet (for example, IP address: 192.168.11.10 and subnet mask: 255.255.255.0)



2. Launch your web browser and enter the IP address of the controller into the address field. The SIL WAC AX has a default IP address of either 192.168.1.2 or 192.168.11.1



3. Enter **admin** in the Username field and **admin** in the Password field and click **Login**.

Username

Password

English (US)

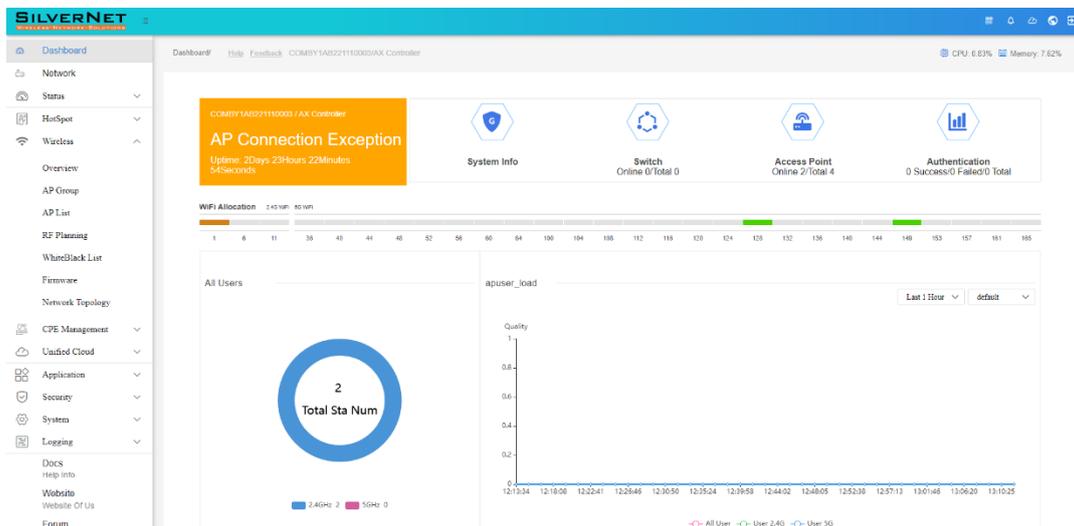
FORGOT PASSWORD ?

LOG IN

SYSTEM OVERVIEW

DASHBOARD

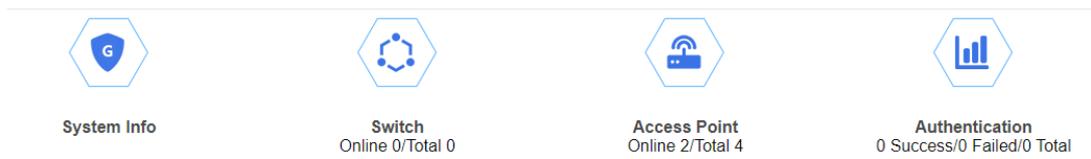
The Dashboard displays a summary of the controller status information, Total number of users, AP load and online devices.



NETWORK STATUS

You can check some basic system info, get some information on the connected AP's and Authentication by hovering your mouse over the blue icons and by clicking them.

The pages they open will be covered later in the manual.



NETWORK

Click on the network tab to configure the IP address of the controller.

The screenshot displays the SilverNet web interface for configuring the LAN interface. The sidebar on the left contains a navigation menu with the following items: Dashboard, Network (selected), Status, HotSpot, Wireless, CPE Management, Unified Cloud, Application, Security, System, and Logging. Below the main menu are links for Docs, Help Info, Website, Website Of Us, Forum, and Forum for Users. The main content area is titled 'Network/Interface' and shows the configuration for the 'LAN' interface. The configuration fields are as follows:

- MAC Address: 50:11:eb:11:00:00
- IP Protocol: DHCP Static
- IP Address: 192.168.168.7
- Netmask: 255.255.255.0
- Gateway: 192.168.168.2
- DNS: 192.168.168.253

A 'CONFIRM' button is located at the bottom of the configuration area.

General Setup

IP Protocol Here you can enable **DHCP Client** or **Static**

DHCP Client If enabled, your device will get an IP address automatically from the network. There must be a DHCP server configured on your network for this to function.

Static Allows you to enter a static IP address.

IP Address Enter the IP address you wish to give to the device. You will use this IP address to access the device interface.

Netmask Enter the class for the IP address. The default is a class C value of 255.255.255.0

Gateway (optional) Enter the gateway IP address of the network the device is connected to.

DNS Enter the IP address for the DNS server you wish to use.

STATUS

WiFi STA INFO

Click on WiFi Sta Info for a detailed list of connected end users.

Configure	IP Address	MAC Address	Hostname	Band	Associated AP	Associated AP Name	MAC Of AP	SSID	Uptime	Signal	RX Rate	TX Rate
Kick	0.0.0.0	90:46:6c:90:7b:ab	*	5G	CDUTD00122A190001	MainOffice	44:d1:fa:e0:91:ec	SilverNet	34Days 0Hours 5Minutes 18Seconds	-46 dBm	72.0	72.0
Kick	0.0.0.0	5c:47:5a:2a:91:52	*	5G	CDUTD00122A190001	MainOffice	44:d1:fa:e0:91:ec	SilverNet	34Days 0Hours 5Minutes 18Seconds	-74 dBm	39.0	72.0
Kick	192.168.168.141	d0:53:49:6d:1a:56	*	2.4G	CDUTD001225170005	Boardroom	44:d1:fa:b2:4a:63	SilverNet	34Days 0Hours 4Minutes 48Seconds	-41 dBm	72.0	65.0
Kick	0.0.0.0	4e:d1:fa:e0:91:f2	*	2.4G	CDUTD00122A190001	MainOffice	44:d1:fa:e0:91:ec	CasinoTest	33Days 23Hours 50Minutes 7Seconds	-95 dBm	65.0	65.0
Kick	192.168.168.58	5c:47:5a:2f:69:1e	*	2.4G	CDUTD001225170005	Boardroom	44:d1:fa:b2:4a:63	SilverNet	25Days 23Hours 40Minutes 0Seconds	-60 dBm	65.0	65.0
Kick	192.168.168.51	9c:76:13:c4:4b:16	*	5G	CDUTD00122A190001	MainOffice	44:d1:fa:e0:91:ec	SilverNet	25Days 23Hours 30Minutes 21Seconds	-68 dBm	1.0	72.0
Kick	192.168.168.61	78:a3:6d:0f:e5:00	*	2.4G	CDUTD001225170005	Boardroom	44:d1:fa:b2:4a:63	SilverNet	24Days 1Hours 34Minutes 54Seconds	-74 dBm	65.0	65.0
Kick	0.0.0.0	22:3d:53:c8:87:a9	*	5G	CDUTD00122A190001	MainOffice	44:d1:fa:e0:91:ec	SilverNet	7Days 5Hours 48Minutes 32Seconds	-46 dBm	173.1	192.1
Kick	192.168.168.67	f0:82:c0:4c:ea:ed	*	2.4G	CDUTD001225170005	Boardroom	44:d1:fa:b2:4a:63	SilverNet	4Days 0Hours 17Minutes 30Seconds	-41 dBm	6.0	72.0
Kick	192.168.168.54	c8:89:f3:a9:5a:99	*	5G	CDUTD00122A190001	MainOffice	44:d1:fa:e0:91:ec	SilverNet	6Hours 41Minutes 38Seconds	-55 dBm	115.1	192.1
Kick	192.168.168.53	06:42:67:c2:33:94	*	5G	CDUTD00122A190001	MainOffice	44:d1:fa:e0:91:ec	SilverNet	6Hours 40Minutes 7Seconds	-71 dBm	39.0	130.1
Kick	0.0.0.0	d6:fb:26:d9:3c:eb	*	5G	CDUTD00122A190001	MainOffice	44:d1:fa:e0:91:ec	SilverNet	6Hours 23Minutes 18Seconds	-51 dBm	52.0	144.1
Kick	192.168.168.65	06:16:6b:73:15:a6	*	5G	CDUTD001225170005	Boardroom	44:d1:fa:b2:4a:63	SilverNet	19Minutes 37Seconds	-61 dBm	24.0	585.5

Configure Clicking Kick will disconnect the end user device for a short period of time, after which the user can reconnect.

IP Address The IP address of the end user device.

MAC address The MAC address of the end user device.

Host Name The name of the end user device.

Associated AP The name of the AP that the end user is connected to.

MAC of AP The MAC address of the AP that the end user is connected to.

SSID The SSID name of the wireless connection the end user is connected to.

Uptime The network connection time of the end user.

Signal The current signal strength of the end users connection to the AP.

RX/TX rate The connection rate of the wireless device.

LINE MONITORING

Interface Status



0: lan

Line Monitoring

Q Input Content AUTO REFRESHING REFRESH

Details	Interface	Port Name	Status	IP Address	IPv6 Address	Sessions	RX rate	TX rate	TX bytes	RX bytes	TX packets(dropped/total)	RX packets(dropped/total)
Details	lan	eth0	Enable	192.168.168.7/255.255.255.0	-	-			0 B	0 B	undefined / undefined	undefined / undefined

Records per page: 20 1-1 of 1 < >

Details Click details to view the line monitoring details.

Interface The name of the selected interface.

Port Name The name of the selected port.

Status Green is Enabled and red is Disabled.

IP address The IP address of the selected interface.

IPv6 Address The IPv6 address of the selected interface.

Sessions The number of sessions.

RX/TX rate The connection rate of the selected interface.

RX/TX bytes The volume of data, in bytes, transmitted via the selected interface.

RX/TX packets The dropped and total packets of the selected interface.

AUTHORISED USERS

A list of authenticated users that have connected via the portal.

Configure		IP Address	IPv6 Address	MAC Address	Username	Authentication Method	Uptime	Session Num
Kick	Block	172.17.17.139	fe80:1071:a58d:b58:ae6c	80:80:3e:38:10:5a		lan	1Minutes 55Seconds	28

Records per page: 20 | 1-1 of 1 | < >

Configure Clicking Kick will disconnect the end user device. The user will need to re-authenticate to access the internet. Clicking Block will Move the end user device to the Blacklist and block the device from connecting to the network.

***You can remove a user from the Blacklist by going to HotSpot-Blacklist**

IP Address The IP address of the end user device.

IPv6 Address The IPv6 address of the end user device.

MAC address The MAC address of the end user device.

Host Name The name of the end user device.

Authentication Method The Method of authentication.

Uptime The network connection time of the end user.

Session Number The session number of the end user.

LICENSE

Here you can view the license information of the controller.

ARP LIST

ARP (address Resolution Protocol) is a TCP/IP protocol that connects a physical address to an IP address. When a computer or mobile phone sends a message, it broadcasts the ARP request containing the target IP address to all devices on the local network. Once it receives a reply it will then be able to determine the target physical address and will store the information in the local ARP cache for a period of time. This will save time for any future requests as it will query the ARP cache first.

IPV4 IPV6

Q Input Content EXPORT REVERSE

<input type="checkbox"/>	Interface Associated	Device IP	Device MAC	Type
<input type="checkbox"/>	br-lan	192.168.168.123	44:d1:fa:b2:4a:63	REACHABLE
<input type="checkbox"/>	br-lan	192.168.168.253	00:15:5d:01:81:02	STALE
<input type="checkbox"/>	br-lan	192.168.168.12	b8:ca:3a:72:8b:75	REACHABLE
<input type="checkbox"/>	br-lan	192.168.168.52	44:d1:fa:e0:91:ec	REACHABLE
<input type="checkbox"/>	br-lan	192.168.168.71	04:bf:1b:32:9e:d7	STALE
<input type="checkbox"/>	br-lan	192.168.168.2	00:1e:42:55:07:e8	REACHABLE

Records per page: 20 1-6 of 6 < >

HOTSPOT

This is where you can create a guest network with varied levels of authentication and billing plans.

LOCAL PORTAL

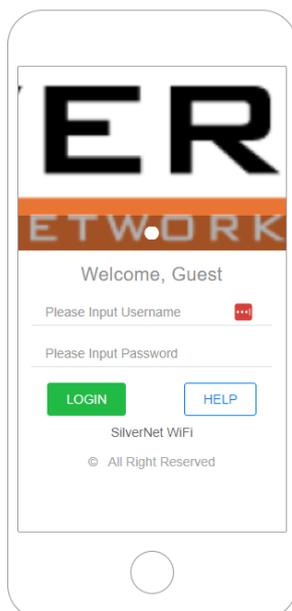
Here you can enter the details for your landing display.

DISPLAY CONFIGURATION

Display configuration

Welcome	<input type="text" value="Welcome, Guest"/>
Contact information	<input type="text" value="SilverNet WiFi"/>
Copyright information	<input type="text" value="All Right Reserved"/>
Login Button Prompt	<input type="text" value="Login"/>
Help Button Prompt	<input type="text" value="Help"/>
Images	<p>Picture size not exceeding 200K, names should not contain special characters such as spaces</p> <p>0 (0.0 B) +</p> <div style="border: 1px dashed gray; padding: 5px; display: inline-block;">  </div>

This phone image will show you a preview of what the display will look like.



AUTHENTICATION CONFIGURATION – LOCAL USER

Here you can configure the Authentication method.

Authentication Configuration

Authentication Method	<input type="text" value="Local User Auth"/>
Self Service Portal	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Self Service Portal Tips:	<input type="text" value="Self-Service"/> <small>Tip: The local self-service Portal path is /user</small>
Redirect Url after Athh success	<input type="text" value="http://www.silvernet.com"/> <small>Url, for example: http://www.example.com/</small>
Auth Validity Time	<input checked="" type="radio"/> Minutes <input type="radio"/> Hours <input type="radio"/> Days <input type="text" value="1"/> <small>No more than 30 days</small>

Authentication Method Local User Authentication.

Self Service Portal Enable or Disable. We recommend to disable.

Self Service Portal Tips Self service button tips.

*Self Service portal is where the customer can go through to a webpage, create and accounts and purchase additional internet time themselves. The account will show in local users.

Redirect URL after Authentication Success Enter the URL of the landing page once the user is authenticated.

Authentication validity Time The amount of time the users session is valid for.

AUTHENTICATION CONFIGURATION – RADIUS AUTH

Here you can configure the Authentication method.

Authentication Configuration

Authentication Method	<input type="text" value="RADIUS Auth"/>
Self Service	<input type="text" value="http://www.example.com"/> <small>Url, for example: http://www.example.com/</small>
Redirect Url after Athh success	<input type="text" value="http://www.silvernet.com"/> <small>Url, for example: http://www.example.com/</small>
Auth Validity Time	<input checked="" type="radio"/> Minutes <input type="radio"/> Hours <input type="radio"/> Days <input type="text" value="1"/> <small>No more than 30 days</small>

Authentication Method RADIUS Auth.

Self Service Enter the Self Service URL.

Redirect URL after Athh success Enter the URL of the landing page once the user is authenticated.

Authentication validity Time The amount of time the users session is valid for.



AUTHENTICATION CONFIGURATION – PHONE NUM AUTH

Here you can configure the Authentication method.

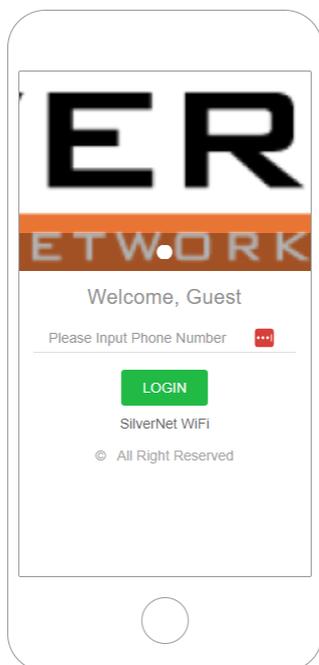
Authentication Configuration

Authentication Method	<input type="text" value="Phone Num Auth"/>
	<input type="button" value="EXPORT PHONE NUMBER"/> <input type="button" value="CLEAN PHONE NUMBER"/>
Redirect Url after Athh success	<input type="text" value="http://www.silvernet.com"/> <small>Url, for example: http://www.example.com/</small>
Auth Validity Time	<input checked="" type="radio"/> Minutes <input type="radio"/> Hours <input type="radio"/> Days <input type="text" value="1"/> <small>No more than 30 days</small>
	<input type="button" value="CONFIRM"/> <input type="button" value="CANCEL"/>

Authentication Method Phone Num Auth.

Redirect URL after Athh success Enter the URL of the landing page once the user is authenticated.

Authentication validity Time The amount of time the users session is valid for.



AUTHENTICATION CONFIGURATION – SMS AUTH

Here you can configure the Authentication method.

Authentication Configuration

Authentication Method: SMS Auth

EXPORT PHONE NUMBER CLEAN PHONE NUMBER

Redirect Url after Athh success: http://www.silvernet.com

Url, for example: http://www.example.com/

Auth Validity Time: Minutes Hours Days

1

No more than 30 days

CONFIRM CANCEL

Authentication Method SMS Auth.

Redirect URL after Athh success Enter the URL of the landing page once the user is authenticated.

Authentication validity Time The amount of time the users session is valid for.



AUTHENTICATION CONFIGURATION – ONEKEY AUTH

Here you can configure the Authentication method.

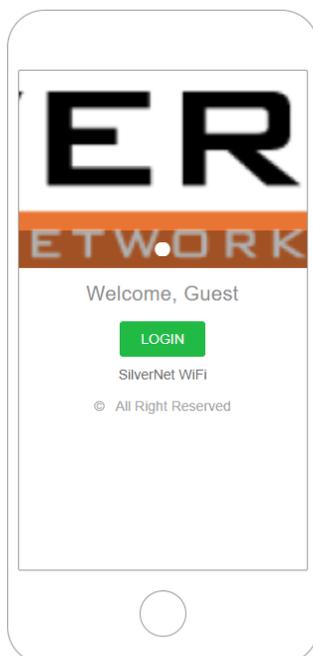
Authentication Configuration

Authentication Method	<input type="text" value="OneKey Auth"/>
Redirect Url after Athh success	<input type="text" value="http://www.silvernet.com"/> <small>Url, for example: http://www.example.com/</small>
Auth Validity Time	<input checked="" type="radio"/> Minutes <input type="radio"/> Hours <input type="radio"/> Days <input type="text" value="1"/> <small>No more than 30 days</small>
<input type="button" value="CONFIRM"/> <input type="button" value="CANCEL"/>	

Authentication Method OneKey Auth.

Redirect URL after Athh success Enter the URL of the landing page once the user is authenticated.

Authentication validity Time The amount of time the users session is valid for.



AUTHENTICATION CONFIGURATION – PRE-SHARED PASSWORD

Here you can configure the Authentication method.

Authentication Configuration

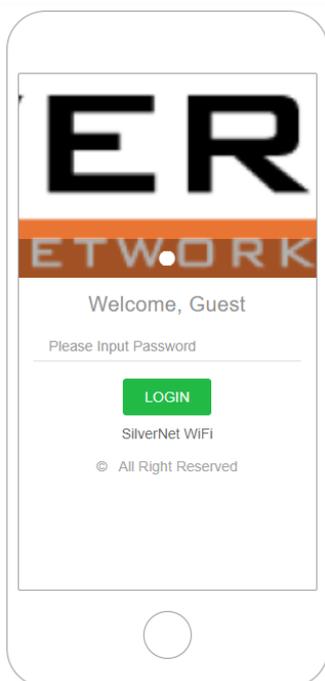
Authentication Method	Pre-Shared Password ▼
Password ⋮ 🔒
Redirect Url after Athh success	http://www.silvernet.com
	<small>Url, for example: http://www.example.com/</small>
Auth Validity Time	<input checked="" type="radio"/> Minutes <input type="radio"/> Hours <input type="radio"/> Days
	<input type="text" value="1"/>
	<small>No more than 30 days</small>
	<input type="button" value="CONFIRM"/> <input type="button" value="CANCEL"/>

Authentication Method Pre-Shared Password.

Password Enter the Pre-Shared Password.

Redirect URL after Athh success Enter the URL of the landing page once the user is authenticated.

Authentication validity Time The amount of time the users session is valid for.



AUTHENTICATION CONFIGURATION – VOUCHERS

Here you can configure the Authentication method.

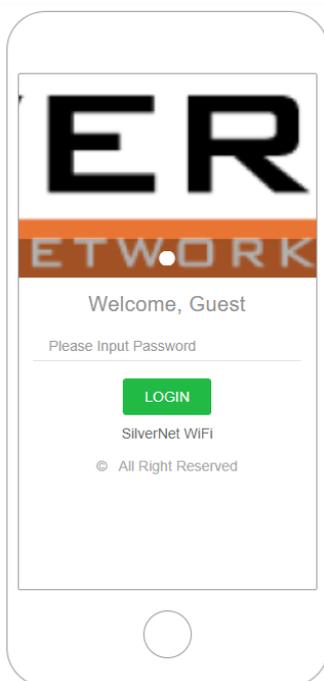
Authentication Configuration

Authentication Method	<input type="text" value="Vouchers"/>
Redirect Url after Athh success	<input type="text" value="http://www.silvernet.com"/> <small>Uri, for example: http://www.example.com/</small>
Auth Validity Time	<input checked="" type="radio"/> Minutes <input type="radio"/> Hours <input type="radio"/> Days <input type="text" value="1"/> <small>No more than 30 days</small>
<input type="button" value="CONFIRM"/> <input type="button" value="CANCEL"/>	

Authentication Method Vouchers.

Redirect URL after Athh success Enter the URL of the landing page once the user is authenticated.

Authentication validity Time The amount of time the users session is valid for.



BILLING PLAN

Billing plan is used with Local Portal.

<input type="checkbox"/>	Configure	Plan Name	Available Time	Self Service	Upload Speed(Kbps)	Download Speed(Kbps)
<input type="checkbox"/>	Edit	Default	Long-term	Disable	2000	2000
<input type="checkbox"/>	Edit	Test1	1Minutes	Enable	200	200

Records per page: 20 ▾ 1-2 of 2 < >

Click the Add button to add a new billing plan.

Plan Name

Unit Minute Hour Day Month

Available Time
0 means No Limit

Upload Speed(Kbps)

Download Speed(Kbps)

Self Service Enable Disable

Plan Name Enter the name of the billing plan.

Unit Select the unit of time.

Available Time Set the Time limit. 0 means there is no limit.

Upload Speed (Kbps) Enter the upload speed limit in Kbps.

Download Speed (Kbps) Enter the download speed limit in Kbps.

Self Service Enable or Disable.

LOCAL USERS

This is where you can set up a general login, Local users or long term guests.

Configure	Status	Username	Password	Auth Protocol	Upload Speed(Kbps)	Download Speed(Kbps)	Due Time	Billing Plan	Remarks
<input type="checkbox"/>	Normal	yourname	yourpasswd	pptp / l2tp / pppoe / webportal	2000	2000	Long-term	Custom	-

Records per page: 20 1-1 of 1

Click Add or edit to begin making changes.

Username

Password

Amount of Concurrency

Note: At the same time, how many users using same account can login, default to 1, 0 means no limit

SMS Notification Enable Disable

Note: When selected, the account information will be sent to the user

Remarks

Plan Select

Upload Speed(Kbps)

Download Speed(Kbps)

Due Time Long-term

Username Enter a username.

Password Enter a password.

Amount of Concurrency Set the maximum number of users that are allowed to login at the same time on the same account. 0 means there is no limit.

SMS Notification Enable or Disable. If enabled will need to configure SMS Gateway.

Remarks Add a remark.

Plan Select You can select any template that you have created in the Billing Plan section.

Upload/Download Speed (Kbps) Enter the upload/download speed limit in Kbps. If using a template it will follow template rules.

Due Time This is the expiry time of the account. Click long term to disable the expiry.

VOUCHERS

This is where you can create vouchers for end users. Ideal for a Hotel scenario.

Click Batch Add.

Code length	<input type="text" value="6"/>
Amount	<input type="text" value="10"/>
Amount of Concurrency	<input type="text" value="1"/>
	<small>Note: At the same time, how many users using same account can login, default to 1, 0 means no limit</small>
Remarks	<input type="text" value="Input Remarks"/>
Upload Speed(Kbps)	<input type="text" value="10000"/>
Download Speed(Kbps)	<input type="text" value="100000"/>
Available Time	<input type="text" value="1 Day"/>
Unit	<input type="radio"/> Minutes <input type="radio"/> Hours <input checked="" type="radio"/> Day <input type="radio"/> Month
	<input type="button" value="CONFIRM"/> <input type="button" value="CANCEL"/>

Code Length This will be the length of the code.

Amount Enter the amount of vouchers you wish to populate.

Amount of Concurrency Set the maximum number of users that are allowed to login at the same time on the same account. 0 means there is no limit.

Remarks Add a remark.

Upload/Download Speed (Kbps) Enter the upload/download speed limit in Kbps.

Available Time/Unit This is the length of the voucher.

Once confirmed the list will appear as below.

Q Input Content		<input type="button" value="BATCHADD"/> <input type="button" value="IMPORT"/> <input type="button" value="EXPORT"/> <input type="button" value="ADVANCED"/> <input type="button" value="PRINT"/> <input type="button" value="CLEAN EXPIRED USER"/> <input type="button" value="REVERSE"/> <input type="button" value="DELETE"/>						
<input type="checkbox"/>	Status	Vouchers	Due Time	Upload Speed(Kbps)	Download Speed(Kbps)	Remarks		
<input type="checkbox"/>	Normal	95489	1Day	10000	100000			
<input type="checkbox"/>	Normal	89830	1Day	10000	100000			
<input type="checkbox"/>	Normal	16317	1Day	10000	100000			
<input type="checkbox"/>	Normal	98275	1Day	10000	100000			
<input type="checkbox"/>	Normal	48965	1Day	10000	100000			
<input type="checkbox"/>	Normal	42203	1Day	10000	100000			
<input type="checkbox"/>	Normal	69314	1Day	10000	100000			
<input type="checkbox"/>	Normal	90277	1Day	10000	100000			
<input type="checkbox"/>	Normal	71872	1Day	10000	100000			
<input type="checkbox"/>	Normal	24563	1Day	10000	100000			

Records per page: 20 1-10 of 10 < >

RADIUS

This is where you can set up Radius Authentication.

RADIUS Server Domain	<input type="text" value="Input RADIUS Server Domain"/> <small>e.g, 192.168.9.250 or www.example.com</small>
Pre-Shared Key	<input type="text" value="max length is 255"/> <small>Pre-Shared Key used to communicate with RADIUS server</small>
Account Port	<input type="text" value="Input Non-zero Number, 0 means No Limit"/> <small>accountingport_help</small>
Auth Port	<input type="text" value="e.g, 1812"/> <small>authenport_help</small>
NAS Identifier	<input type="text" value="Input NAS Identifier"/> <small>IP or NAS Token</small>
Bind IP	<input type="text" value="IP Address Bind(Optional), like 192.168.100.100"/> <small>IP used to communicate with RADIUS Server</small>
Connection Status	<p style="color: red;">Connection Failed </p>

Radius Server Domain Enter your Radius server IP address.

Pre-Shared Key Enter the Radius server Pre-Shared Key.

Account Port Enter the Radius server account port number.

Auth Port Enter the Radius server Authentication port number.

NAS Identifier IP address of the network access server (NAS) that requests user authentication.

Bind IP Optional IP address to Bind to.

Once the information has been entered you can test the connection and then confirm.

SMS GATEWAY

This is where you can select the SMS Gateway. Currently we only support Clickatell, AliDaYu and Ihuyi.

SMS-Gateway Clickatell AliDaYu ihuyi

Account
username of ihuyi

Password
password of ihuyi

SMS Template for Account Creating ⋮

SMS Template for Due Notice ⋮

SMS Template for Verification

CONFIRM

Enter your account details to enable SMS.

WHITE LIST

[IP WHITE LIST](#) [DOMAIN WHITE LIST](#)

ADD BATCHADD REVERSE DELETE

<input type="checkbox"/>	Configure	IP Address	Remarks
⚠ No data available			

Select IP or Domain white list, and click the add or batch add button to fill in address. Any IP entered here will not need to Authenticate.

BLACK LIST

[IP BLACK LIST](#) [DOMAIN BLACK LIST](#)

ADD BATCHADD REVERSE DELETE

<input type="checkbox"/>	Configure	IP Address	Remarks
⚠ No data available			

Select IP or Domain Black list, and click the add or batch add button to fill in address. Any Ip address entered here will not be able to access the network.

WIRELESS

OVERVIEW

Global Config

Access Controller	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AC-AP Time Sync	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Auto Upgrade	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
AP Scheduled Reboot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Daily
AP Scheduled Reboot Time	<input type="text"/> * <small>The device will not restart again if it runs for less than one hour</small>
AC Scheduled Reboot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Daily
AC Scheduled Reboot Time	<input type="text"/> * <small>The device will not restart again if it runs for less than one hour</small>
Wireless Optimization	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Watchdog	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Destination Address	<input type="text" value="Input Destination Address"/> <small>Note: If the Address Do not Alive, AP will Open Rescue Network Automaticly (SSID: RESCUE_99_XXXX,Password: 99999999)</small>
Country For All AP	United Kingdom <input type="button" value="CONFIRM"/>

Access Controller Select Enable or Disable.

AC-AP Time Sync Select Enable or Disable.

AP Auto Upgrade Select Enable or Disable.

AP Scheduled Reboot Select Enable or Disable. If Enabled, select if the schedule will be Daily, Weekly or Monthly and then Select the Day of the week or Month.

AP Scheduled Reboot Time Select the time you wish the AP's to be rebooted.

AC Scheduled Reboot Select Enable or Disable. If Enabled, select if the schedule will be Daily, Weekly or Monthly and then Select the Day of the week or Month.

AC Scheduled Reboot Time Select the time you wish the AC to be rebooted.

Wireless Optimisation Select Enable or Disable.

AP Watchdog Select Enable or Disable. Input the address of the AP's you wish to monitor. If the AP is offline it will go into rescue mode with details of (SSID: RESCUE_99_XXXX,Password: 99999999)

Country For All AP Select the country code you wish to use.

AP GROUP

This is where you can create AP groups

Search:

[ADD](#) [REVERSE](#) [DELETE](#)

<input type="checkbox"/>	Configure	Group Name	AP Num	WxApp Support
<input type="checkbox"/>	Edit	default	0	Disable
<input type="checkbox"/>	Edit	Group1	2	Disable

Records per page: 20 ▾ 1-2 of 2 < >

Click the Add button to add a group or edit to edit a current group.

Group Name

[2.4GHz](#) [5GHz](#) [Other Configuration](#)

Group Name Enter a name for the Group.

Select 2.4GHz, 5GHz or Other configuration to edit those settings.

2.4GHZ

Configure your 2.4Ghz settings.

Wireless Template Configuration

[Add](#)

1

SSID	<input type="text" value="Input SSID"/>
Encryption	<input type="text" value="Open"/> ▼
Advance Features	<input type="checkbox"/> Isolate <input type="checkbox"/> Hidden <input type="checkbox"/> Qrcode
MAX Num of User	<input type="text" value="0"/>
AuthType	<input type="text" value="None"/> ▼
VLAN BINDING	<input type="text" value="0"/>

[Delete](#)

Advanced ▼

CONFIRM

GO BACK

SSID Enter the SSID. This will be visible to other devices.

Encryption Select your encryption method.

Advanced features Select if needed. **Isolate** will stop any user devices connected to this Wi-Fi from communicating with each other. **Hidden** will hide the SSID so that it is not visible.

Max Num of User Enter the maximum number of users or leave at 0 for unlimited.

Authentication Type Select None or Local Portal.

VLAN Binding Enter a VLAN ID if using VLANS.

***Note – If you need more than one SSID, click Add and you can create multiple.**

5GHz

Configure your 5Ghz settings.

Wireless Template Configuration

[Add](#)

1

SSID	<input type="text" value="Input SSID"/>
Encryption	<input type="text" value="Open"/> ▼
Advance Features	<input type="checkbox"/> Isolate <input type="checkbox"/> Hidden <input type="checkbox"/> Qrcode
MAX Num of User	<input type="text" value="0"/>
AuthType	<input type="text" value="None"/> ▼
VLAN BINDING	<input type="text" value="0"/>

[Delete](#)

Advanced ▼

CONFIRM

GO BACK

SSID Enter the SSID. This will be visible to other devices.

Encryption Select your encryption method.

Advanced features Select if needed. **Isolate** will stop any user devices connected to this Wi-Fi from communicating with each other. **Hidden** will hide the SSID so that it is not visible.

Max Num of User Enter the maximum number of users or leave at 0 for unlimited.

Authentication Type Select None or Local Portal.

VLAN Binding Enter a VLAN ID if using VLANS.

***Note – If you need more than one SSID, click Add and you can create multiple.**

ADVANCED

Here you can configure some advanced settings.

Advanced ^

Channel	<input type="text" value="AUTO"/>
Roaming Threshold	<input type="text" value="-95"/>
U-APSD	<input checked="" type="checkbox"/> Enable <small>U-APSD is a new energy-saving processing mode, which can enhance the terminal energy-saving capacity. However, due to the problems in supporting U-APSD functions in some terminals, it is necessary to turn off U-APSD functions in this case.</small>
FILS Support	<input checked="" type="checkbox"/> Enable <small>Support 802.11ai, fast initial link setup. Reduce the waiting time for networking to less than 100 ms</small>
802.11kvr Roaming	<input type="checkbox"/> Enable <small>Enable Fast Roaming between access points in the group. Note that it is only valid in encrypted cases</small>
RTS Threshold	<input type="text" value="2347"/> <small>Resolve wireless data conflicts. When the data length exceeds this value, the wireless access point needs to send the RTS signal to the station, then receive the feedback from the station, before sending the data</small>
Signal	<input type="text" value="AUTO"/>
Channel Bandwidth	<input type="text" value="AUTO"/>
5GHz First	<input checked="" type="checkbox"/> Enable <small>Note: When the Configuration of 2.4GHz and 5GHz is the same, WiFi User will preferentially connect to 5GHz WiFi</small>
WMM	<input checked="" type="checkbox"/> Enable
GBK SSID	<input type="checkbox"/> Enable <small>Enable GBK can solve the problem that some station (computers, etc.) do not display wireless ssid property</small>
WhiteBlack List	<input type="text" value="....."/>

Channel Select the channel for your WiFi. We recommend leaving on Auto.

Roaming Threshold When a users device fall below this threshold it will automatically disconnect and roam to the next AP. Setting depends on the environment, but the recommended range is -80 to -85.

U-APSD Select Enable or Disable. U-APSD stands for Unscheduled Automatic Power Save Delivery. It is a power saving setting. When enabled any AP that does not have anything to transmit will go into standby mode checking for traffic every 100 to 200ms. Once it has something to transmit it will wake up.

This setting is fine for web browsing or emails, however, if you experience any problems then it is best to disable the setting.

FILS Support Select Enable or Disable. FILS stand for Fast Initial Link Setup. It reduces the link up time to below 100ms. Designed for dense environments.

802.11kvr Roaming Select Enable or Disable. When Enabled it allows clients to roam more seamlessly from AP to AP within the same network.

RTS Threshold Set the RTS (Request To Send) packet size. Default is 2347 octets. It is recommended to leave this setting.

Signal Set the power levels. It is recommended to leave this setting on Auto.

Channel bandwidth Set the channel size. It is recommended to leave this setting on Auto.

5GHz First Select Enable or Disable. When the configuration of 2.4GHz and 5GHz is the same, this setting will push users onto the 5GHz frequency first.

WMM Select Enable or Disable. When enabled WMM prioritises network traffic to improve performance of applications such as video and voice.

GBK SSID Select Enable or Disable. Enabling this setting can sometimes solve an issue where by some computers do not display the SSID correctly.

WhiteBlack list In White List mode, only the MAC addresses in the White list can access the WiFi. In Blacklist mode, only the MAC address in the Blacklist cannot access the WiFi. This setting is configured in its own tab. See further below.

OTHER CONFIGURATION

Configure your WiFi Schedule

Basic Configuration

WiFi Schedule	<input checked="" type="checkbox"/> Enable
Repeat	<input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday <input type="checkbox"/> Sunday
Start Time	<input type="text" value="00:25"/> 
Stop Time	<input type="text" value="01:00"/> 

WiFi Schedule Enable or Disable.

Repeat Select the days you want your WiFi Schedule to operate.

Start Time Select the start time.

Stop Time Select the end time.

AP LIST

AP List shows you the current AP's connected to the controller. To connect an AP you will need to power on the AP and make sure it is connected to the same network as the controller. Once the controller discovers the AP then it will appear as online.

<input type="button" value="AUTO REFRESHING"/> <input type="button" value="OVERVIEW"/> <input type="button" value="REVERSE"/> <input type="button" value="RESTART AP"/> <input type="button" value="BIND"/> <input type="button" value="UNBIND"/> <input type="button" value="NETWORK CONFIG"/> <input type="button" value="SET TXPOWER"/> <input type="button" value="SET CHANNEL"/> <input type="button" value="SET BANDWIDTH"/> <input type="button" value="SET AC ADDRESS"/> <input type="button" value="EXPORT AP INFO"/>											
<input type="button" value="UPGRADE"/> <input type="button" value="SYNC LOGIN PASSWORD"/> <input type="button" value="REFRESH"/>											
<input type="checkbox"/>	Model	Online State	Device Name	IP Protocol	Manager	Apmode	IP Address	MAC Address	Uptime	AP Group	Last Updated
<input type="checkbox"/>	SIL-WAC-AX	Online	Boardroom	static	Local Admin	FIT_AP	192.168.168.123	44:d1:fa:b2:4a:63	34Day 23h16m	Group1	13-02-2024 14:01
<input type="checkbox"/>	SIL-WAC-AX-EXT	Online	MainOffice	static	Local Admin	FIT_AP	192.168.168.52	44:d1:fa:e0:91:ec	34Day 23h8m	Group1	13-02-2024 14:01

Records per page: 20 | 1-2 of 2 | < >

BINDING

To add the online AP into the Group you simply select the AP and Click Bind. Once the AP is in the Group it will show under the AP Group column.

To unbind or to use any of the others settings (like set txpower, set channel, etc) simply select the AP and click the setting.

RF PLANNING

RF Planning can be used to scan and adjust channels.

2.4G AP:0 Dual-Band AP:2 Offline Device:0

INIT CHANNELS START SCAN SAVE RESULT

Configure	SN	Online State	Plan Status	MAC Address	2.4G Channel	5G Channel	2.4G Noise	5G Noise	2.4G Interference	5G Interference
View	CDUTD001225170005	Online	Init Channels OK	50:11:3b:b2:4a:63	6	128	-95	-95	9	7
View	CDUTD00122A190001	Online	Init Channels OK	50:11:eb:e0:91:ec	11	48	-95	-95	45	41

Records per page: 20 1-2 of 2 < >

INIT Channels Click this to use the channel plan. Save the configuration.

Start Scan This will scan and gather local WiFi information to best plan the RF channels.

Configure Click the View button to show WiFi information.

SN The AP Serial number.

Online State Online or Offline.

Plan Status Shows the initialisation channel status.

MAC Address Shows the MAC address of the AP.

2.4GHz/5GHz Channel Shows the channel number.

2.4GHz/5GHz Noise Shows the roaming threshold.

2.4GHz/5GHz Interference Shows the number of WiFi nearby.

WHITEBLACK LIST

Click Add and choose Black List or White List.

Name	<input type="text" value="Input Name(Max length is 32)"/>
Strategy	<input checked="" type="radio"/> Black List <input type="radio"/> White List
MAC List	<div style="border: 1px solid #ccc; height: 100px;"></div>
<input type="button" value="CONFIRM"/> <input type="button" value="CANCEL"/>	

The MAC addresses in the White list can access the WiFi. The MAC address in the Blacklist cannot access the WiFi.

***Note - One MAC record takes up one line. You can add a note after it if separated by a space, or it can be added with no note.**

e.g., 50:00:00:00:00:01 Router MAC

e.g., 50:00:00:00:00:02

FIRMWARE

To Upgrade the firmware via the controller, the AP's must be bound in a group first.

Model	<input type="text"/>
Version	<input type="text" value="Input Version"/>
Remarks	<input type="text" value="Input Remarks"/>
Firmware	0 (0.0 B) +

Model Select the correct model.

Version Input version.

Remarks Enter any remarks.

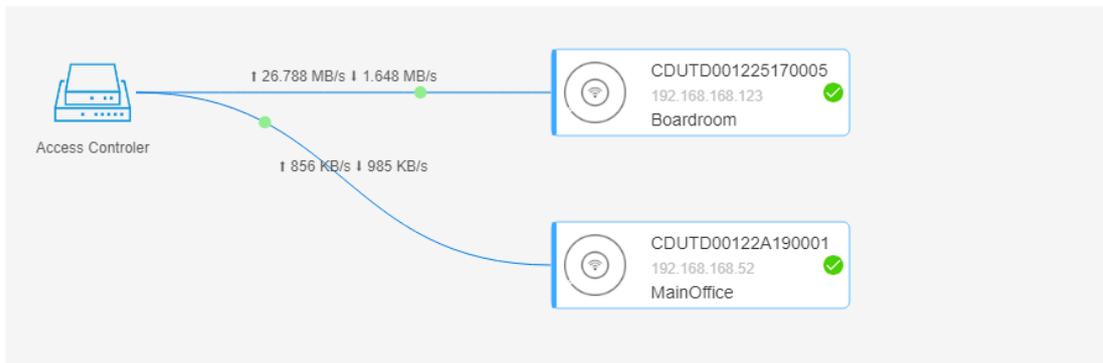
Firmware Click the + sign and browse to the firmware on your local machine.

NETWORK TOPOLOGY

Displays the CPE topology such as link quality, wireless rate, current speed and CPE information in the list.

STA Mode:0 Base Mode:0 Switch:0 Access Point:2 Offline Device:0

ABBREVIATED VIEW DETAILED VIEW EXPORT IMG — Wired - - - - - Wireless



CPE MANAGEMENT

CPE GLOBAL CONFIGURATION

Global Config

CPE Scheduled Reboot Enable Disable
Daily

CPE Scheduled Time *

Wireless Optimization Enable Disable

Transport Scenario Common Scenario Elevator Scenario PTP Scenario Roaming Scenario Custom Scenario

CONFIRM

CPE Scheduled Reboot Enable or Disable. If Enabled, select if the schedule will be Daily, Weekly or Monthly and then Select the Day of the week or Month.

CPE Scheduled Reboot Time Select the time you wish the CPE to be rebooted.

Wireless Optimisation The controller scans for any local interference and automatically assigns channels to the CPE's.

Transport Scenario Select the most suitable scenario.

UNIFIED CLOUD

UNIFIED CLOUD

Unified Cloud is a cloud platform for centralised management of wireless network devices. You can view and manage your devices in the cloud, such as: viewing the status of the devices, modifying the configuration and authentication management.

Serial Number	COMBY1AB221110003
Binding Code	<input type="text" value="Input Binding Code"/>
Longitude	<input type="text" value="Input Longitude"/>
Latitude	<input type="text" value="Input Latitude"/>
Description	SIL-WAC-G3

How to Bind to Unified Cloud

- 1.Login the Unified Cloud Control Platform -> Obtain the Binding Code -> Input the Binding Code and Note Name on Device -> Save and complete the binding.
- 2.Login the Unified Cloud Control Platform -> Add Group -> Add Network --> Add Device -> Input the Serial Number -> Save and complete the binding.

How to manage

After successful binding, about 3 minutes, you can see the device in the Unified Cloud, which can be managed and on Unified Cloud.

How to unbind with Unified Cloud

Login to the Unified Cloud, on the Routing List -> Device Management -> Routing Information Overview Page, you can unbind the device.

APPLICATION

UPNP SERVER

Universal Plug and Play (UPnP) is a standard that lets network devices automatically find, communicate, and control each other. You can enable UPnP in this section.

UPnP Service	<input checked="" type="checkbox"/> Enable
Default WAN Port	<input type="text" value=""/>
Cleanup When Offline	<input checked="" type="checkbox"/> Enable

UPnP Service Enable or Disable.

Default WAN Port WAN

Cleanup When Offline Enable or Disable.

DDNS

Dynamic DNS (DDNS) is a service that can automatically update DNS records when an IP address changes. It connects to the DDNS service providers system with a unique login name and password. Depending on the provider, the host name is registered within a domain owned by the provider or within the customers own domain name. For detailed configuration parameters, please contact the service provider.

Service Provider	<input type="text" value="dyndns.org"/>	
Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Domain	<input type="text" value="www.silvernet.com"/>	*
Account	<input type="text" value="Input Account"/>	*
Password	<input type="text" value="Input Password"/>	*
Protocol	<input type="radio"/> IPv4 <input checked="" type="radio"/> IPv6	
Binding Type	<input type="radio"/> Interface <input checked="" type="radio"/> MAC Address	
Binding Host MAC	<input type="text" value="Input MAC Address"/>	*

Service Provider Select a service provider from the list.

Enable Enable or Disable.

Domain Enter the domain name.

Account Enter the account information.

Password Enter the Password information.

Protocol Select IPv4 or IPv6.

Binding Type Select interface or MAC address.

Binding Host MAC Input the MAC address.

Binding Interface Select the binding interface.

NGROK CLIENT

Ngrok allows you to create a managed tunnel that does not need NAT or port mapping.

Description	<input type="text" value="Input Description"/>
Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
Service Address	<input type="text" value="server.natappfree.cc"/>
Server Port	<input type="text" value="default: 4443"/>
Token	<input type="text" value="Input The unique Token provided by the server"/>
User Domain	<input type="text" value="Input User Domain"/>
Protocol	<input type="text" value="HTTP"/> ▾
Local Address	<input type="text" value="Input Local Address"/>
Local Port	<input type="text" value="Input Local Port"/>

Description Enter a description.

Enable Yes or No.

Service Address Enter the server address.

Server Port Default is 4443

Token Enter the unique token provided by the server.

User Domain Enter the user domain.

Protocol Select HTTP, HTTPS, TCP.

Local Address Input the local address

Local Port Input the local port.

WAKE ON LAN

Wake-on-LAN (WOL) is an Ethernet or token ring computer networking standard that allows a computer to be turned on or awakened by a network message. The message is usually sent to the target computer by a program executed on a device connected to the same local area network, such as a smart phone.

Wake Now

MAC Address

Wake Scheduled

<input type="checkbox"/>	Configure	MAC	Device Status	Cycle	Date	Time	Remarks	Scheduled
⚠ No data available								

Wake Now

MAC Address Enter the MAC address of the device to wake up.

Wake Schedule

MAC *

Cycle ▼

Date 📅 *

Time 🕒 *

Remarks

MAC Enter the MAC address of the device to Wake up.

Cycle Select once, daily, weekly or monthly.

Date Select the date.

Time Select the time.

Remarks Enter any remarks.

SWITCH LINKAGE

Here you can use SNMP to add switches to the controller for management and monitoring.

SMART DEVICE

Here you can use manage and monitor devices like cameras, etc.

SECURITY

EMAIL NOTICE

Email notice only works when using a cloud option. It does not work without access to the cloud.

Event Type

apwarning apdown apreboot
 securitywarning ipconflict netloop

Email List

<input type="checkbox"/>	Configure	Email	Remarks
⚠ No data available			

Click add to enter an email address. Select the Events you wish to receive an email for.

SYSTEM

This section is where you can change the system name, save config files, etc.

SYSTEM MAINTENANCE

System Information

Device Name Enter a name.

Reboot

Uptime Shows the uptime of the controller.

Reboot Click reboot now to reboot the controller.

Online upgrade

Check for new version Will check online for a newer version of firmware.

System Version Displays the current version of firmware.

Model Displays the model number.

Serial Number Displays the serial number.

Menu Upgrade

Local Upgrade Click the + sign and browse to the firmware on your local machine.

Upload Backup File

Last Backup Time Shows the last time a backup configuration file was saved.

Upload Backup file Click the + sign and browse to the configuration file on your local machine.

Backup Configuration Click this to save the current configuration file.

Reset to Factory Click this to reset the controller to its factory default settings.

USER MANAGEMENT

This section allows you to add and remove users.

<input type="checkbox"/>	Configure	Status	Username	Privilege Group	Allowed IP
<input type="checkbox"/>	Edit	Enable	admin	System administrator	0.0.0.0/0

Records per page: 20 1-1 of 1

Click Add to add a new user or Edit to change the administrator details.

Username *

Password

Confirm New Password

Allowed IP
Single address or network (e.g: 172.16.3.2 or 172.16.3.0/24), separate multiple items by space

User Role

Username Enter a username

Password Enter a password

Confirm New Password Re-enter the password.

Allowed IP This allows access to certain IP addresses.

User Role Select the role of the user. Admin account defaults to administrator.

DIAGNOSIS

Here you can run a ping test and a traceroute test.

PING

PING

IP or Domain	<input type="text" value="192.168.168.6"/>	*
Protocol	<input type="text" value="IPv4"/>	▼
Interface	<input type="text" value="ANY"/>	▼
PING Count	<input type="text" value="4"/>	time
Result	<pre>PING 192.168.168.6 (192.168.168.6): 56 data bytes 64 bytes from 192.168.168.6: seq=0 ttl=64 time=2.055 ms 64 bytes from 192.168.168.6: seq=1 ttl=64 time=0.656 ms 64 bytes from 192.168.168.6: seq=2 ttl=64 time=0.649 ms 64 bytes from 192.168.168.6: seq=3 ttl=64 time=0.731 ms</pre>	

IP or Domain Enter the IP address or Domain you wish to ping.

Protocol Select the protocol you wish to use.

Interface Select the interface.

Ping Count Select the amount of pings

Start test Starts the ping test.

TRACEROUTE

Troucert

IP or Domain	<input type="text" value="192.168.168.6"/>
Protocol	<input type="text" value="IPV4"/>
Interface	<input type="text" value="ANY"/>
Result	<pre>tracert to 192.168.168.6 (192.168.168.6), 30 hops max, 46 byte packets 1 192.168.168.6 (192.168.168.6) 0.793 ms 0.660 ms 1.019 ms tracert over!</pre>

[START TESTING](#)

IP or Domain Enter the IP address or Domain you wish to ping.

Protocol Select the protocol you wish to use.

Interface Select the interface.

Start test Starts the ping test.

NETWORK TOOL

Here you can use this section to access the telnet of devices like switches.

TELNET

Telnet

Telnet IP	<input type="text" value="192.168.168.6"/>
Telnet Port	<input type="text" value="23"/>
<input type="button" value="START"/>	

Telnet IP Enter the IP address or Domain you wish telnet to.

Telnet Port Enter the telnet port.

Click start to open the session.

```
Telnet 192.168.168.6 Port 23
connected: ok
*****
  Welcome to the CLI for SilverNet Series 7 product line
        Software Ver: V2.2
*****
Username: █
```

SYSTEM TIME

This is where you can set up your NTP. The Controller automatically updates the system time once it has internet access.

NTP

System Time	<input type="text" value="2024/02/14 15:24:57"/> 
	Sync System Time
NTP Service	<input checked="" type="checkbox"/> Enable NTP
Time Zone	<input type="text" value="Europe/London"/> 
Time Server 1	<input type="text" value="0.pool.ntp.org"/> Sync Now
Time Server 2	<input type="text" value="1.pool.ntp.org"/> Sync Now
Time Server 3	<input type="text" value="2.pool.ntp.org"/> Sync Now
Time Server 4	<input type="text" value="3.pool.ntp.org"/> Sync Now
<input type="button" value="CONFIRM"/>	

System Time Displays the current time.

NTP Service Enable or Disable NTP.

Time Zone Select your time zone.

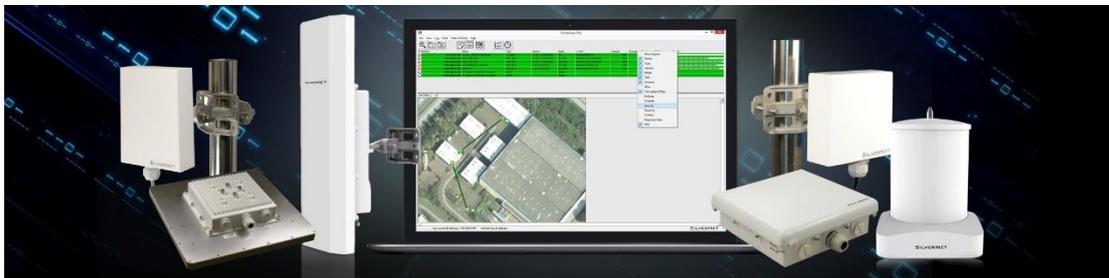
Time Server Enter details of your time server and Sync.

LOGGING

This is where you can see and export any logs for diagnostics.

OTHER SILVERNET PRODUCTS

PRO RANGE



INDUSTRIAL NETWORK TRANSMISSION



INTELLIGENT WI-FI SOLUTIONS



INDUSTRY LEADING TECHNICAL SUPPORT

